[19]中华人民共和国国家知识产权局

[51]Int. Cl[7]
H04L 29/06

[12]发明专利申请公开说明书

[21]申请号 98811413.5

[43]公开日 2001年1月10日

[11]公开号 CN 1279856A

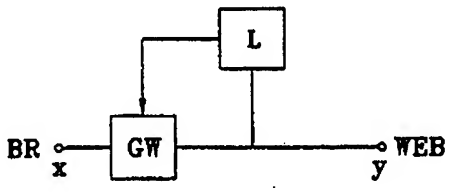
[22]申请日 1998.2.23 [21]申请号 98811413.5
[30]优先权
[32]1997.9.22 [33]IL [31]121815
[86]国际申请 PCT/IL98/00082 1998.2.23
[87]国际公布 WO99/16225 英 1999.4.1
[85]进入国家阶段日期 2000.5.22
[71]申请人 保安-7(软件)有限公司
地址 以色列约克内阿姆
[72]发明人 D·埃尔格雷斯 A·乔斯佩
[74]专利代理机构 中国专利代理(香港)有限公司
代理人 程天正 陈景峻

权利要求书1页 说明书8页 附图页数1页

[54]发明名称 识别和封锁可执行对象的方法和系统

[57]摘要

处理可执行对象的一种方法,包括:(a)提供分析装置,它能够对在浏览器和网上的HTTP服务器之间的通信线路上发送的数据分组进行无干扰的分析,所说的通信线路是通过网关而建立的;(b)分析在上述浏览器和上述服务器之间的联络信号,以检测由用户送出的"GET"命令和由上述服务器作出响应而送出的HTTP代码,(c)当检测到这样的HTTP代码时,分析由上述服务器发送给上述浏览器的数据分组,其过程为:(c.1)提供排序装置以便把收到的无顺序的数据分组排序,然后把它们以顺序的方式转发给标题检查装置;(c.2)检查数据分组以便分析可执行对象的标题的内容并识别它所需要使用的系统资源;(c.3)将表示可执行对象所需要使用的系统资源的数据发送给上述网关;(c.4)提供连接到上述网关的数据分组封锁装置,使得如果按照管理者设置的安全策略不允许使用可执行对象所需要使用的系统资源时,至少一个属于可执行对象的数据分组被封锁、改变或损坏,从而防止它被浏览器所执行。



ISSN1008-4274

权　利　要　求　书

1. 处理可执行对象的一种方法，包括：

(a) 提供分析装置，它能够对在浏览器和网上的 HTTP 服务器之间的通信线路上发送的数据分组进行无干扰的分析，所说的通信线路是通过网关而建立的；

(b) 分析在上述浏览器和上述服务器之间的联络信号，以检测由用户送出的“GET_”命令和由上述服务器作出响应而送出的 HTTP 代码；

(c) 当检测到这样的 HTTP 代码时，分析由上述服务器发送给上述浏览器的数据分组，其过程为：

(1) 提供排序装置以便把收到的无顺序的数据分组排序，然后把它们以顺序的方式转发给标题检查装置；

(2) 检查数据分组以便分析可执行对象的标题的内容，并识别它所需要使用的系统资源；

(3) 将表示可执行对象所需要使用的系统资源的数据发送给上述网关；以及

(4) 提供连接到上述网关的数据分组封锁装置，使得如果按照由管理者设置的安全策略不允许使用可执行对象所需要使用的系统资源时，至少一个属于可执行对象的数据分组被封锁、改变或损坏，从而防止它被浏览器所执行。

2. 按照权利要求 1 的方法，其特征在于还包括识别通过网关进行通信的用户和上述用户所连接的服务器，并且把所有的活动和分析都和上述用户相联系。

3. 按照权利要求 1 和 2 的方法，其特征在于还包括在存储装置中存入表示被分析的可执行对象的校验和，与其一起存放的还有表示任何这样的可执行对象是否符合安全策略的值，并且在分析它之前针对该存放的值去检查任何进入的可执行对象，以此来丢弃任何被判定为不符合安全策略的可执行对象，而让被判定为遵守安全策略的可执行对象通过网关而到达用户。

4. 一种用于实质上如上说明和示例的处理可执行对象的方法。

说　明　书

识别和封锁可执行对象的方法和系统

发明领域

本发明涉及计算机网络的安全管理．更具体说，本发明涉及防止在计算机网络的工作站中下载和执行不希望的可执行对象．

发明背景

自从因特网在几年前创办以来，它在其内容和所采用的技术两方面都已得到很大发展，在因特网早期，站点只包括文本，但随后不久就引入了图形．随站因特网的发展，开发了许多标准，如图象、声音和视频文件，同时也和它们一起开发了用于回放它们的程序（称为“回放程序”）．最初，这些文件只是根据用户的请求才下载到用户的工作站中，并在从用户得到特定命令之后才由相应的回放程序提取．

当随着万维网的自然发展历程而寻找一种能显示更优美、交互和活动的网页的努力开始后，Sun 微系统公司开发了 Java，这是一种能够让网站主人写出一个程序的语言，这个程序是一系列命令，即网络可执行程序，它将在用户不知情的情况下下载到用户工作站并在他的工作站中的浏览器上执行．这种可执行程序用来，例如，在网络冲浪者的屏幕上提供活动图象和别的图形．这样的可执行程序有多种方法接触用户工作站的资源，而这将导致严重的安全问题．虽然在 Java 语言中定义了若干保密级别，但是很快在该语言中发现了巨大的安全漏洞．

在 Java 被开发之后，Microsoft(微软)开发了 ActiveX，它是另一种网络可执行程序的格式，它也是下载到工作站中去的．ActiveX 同样具有相同类型的安全问题．

因特网上充满了“网络可执行程序”，它们可以在用户经过考虑或不知情的情况下下载到各单位的工作站中去．这些代码一般含有无害的功能．尽管它们是安全的，但不一定符合各个单位中所要求的安全策略．

这种代码一旦执行时，它们可能会阻塞网络，导致对局部的数据库、工作站和服务器的可观的不可逆转的损害，或者导致对服务器/工作站的未经授权的信息检索．这样的单元可以存在于 Java 应用软

件、ActiveX 部件、DLL 和其它目标代码中，它们的使用正以无可比拟的速度在增长．这些小程序的大多数是在未经请求和未加控制的情况下下载到单位内的．企业没有办法知道它们的存在和执行，并且现在还没有现成的系统来早期检测和防止这些代码得到执行．

这个安全问题部分地由浏览器的制造商加以解决，它们可以让用户不能使用可执行程序。当然这不是一个合理的解决办法，因为所有的电子商务和广告是以使用可执行程序为基础的．这个安全问题在一旦这种可执行程序能够接触企业的服务器、数据库和其它工作站时将会变得严重得多．

在 1997 年 3 月 10 日提交的共同待审查的专利申请 IL 120420 中，叙述了一种方法（即有选择地防止在计算机中下载和执行不需要的可执行对象），该申请在此引用以供参考，该方法包括以下步骤:

（a）提供一个或多个控制中心，每个都连接到一个或多个网关，每个网关为一个或多个最终用户计算机服务;

（b）提供一种连接到每个上述网关、用于检测到达上述网关的可执行对象、分析每个上述可执行对象的标题、和确定该可执行对象需要使用的计算机资源的装置;

（c）提供一种连接到每个上述网关的装置，用于存储表示资源或资源组合的每个终端用户计算机安全策略，这表示管理者允许或不允许在它的目的地内使用可执行对象，其中该安全策略是从每个上述的一个或多个控制中心收到和/或存储于其中的;

（d）当在网关检测到一个可执行对象时:

1. 分析该可执行对象的标题;

2. 确定该可执行对象需要使用的计算机资源;

3. 将该可执行对象需要使用的计算机资源与安全策略相比较以及

（i） 如果该可执行对象需要使用的计算机资源被包括在安全策略允许使用的资源清单之内，就允许可执行对象通过该网关并到达已经起动其下载操作的计算机; 以及

（ii） 如果该可执行对象需要使用的计算机资源被包括在安全策略禁止使用的资源清单之内，就防止可

执行对象通过该网关，从而防止它到达已经起动了下载操作的计算机上.

控制中心（CC）可以是一个中央控制单元，例如 PC 机或其它计算机，它连接到多个网关，它还更新含有相关数据（例如安全策略）的内存装置. 一旦 CC 通过例如对安全策略增加另外的限制来实行更新时，所有的网关也立即得到更新. 使用 CC 来控制网关的安全单元的操作消除了每次在策略作出改变时要更新每一个网关的需求（这在现有技术的系统中是存在的）.

LAN（局域网）可以是（但并不限于）例如位于一个办公室或一座建筑中的计算机网络. LAN 一般是通过一个或多个网关连接到外部的通信网络（诸如万维网）或者更为局限的 LAN（例如客户或供应者的 LAN）. 单位越大，则为了使通信保持在合理的速度上，所用的网关的数量也越多.

一般说来，LAN 也可以由多个较小的 LAN 组成，它们在地理上靠得很近或相互远离，但是，即使在同一个单位内建立了小型的 LAN，安全要求也可能随不同的部门而有不同变化，而且有可能要保持较高的安全级别，包括即使在同一单位内也要防止可执行程序从一个部门转移到另一部门.

所述连接到每个上述网关、用于检测到达上述网关的可执行对象、分析每个上述可执行对象的标题、和确定可执行对象需要使用的计算机资源的装置可以是有许多不同类型的. 一般说来，可执行对象是通过在通信线路上侦听 TCP/IP 协议、而且也侦听像 SMTP、HTTP、FTP 等目标传输协议而在网关上被“捕捉”和分析的. 和通信线路相连接和从可执行对象中摘取标题的内容这样的步骤是熟练技术人员都知道的，而且它们都可以用传统的编程来实现，因此，为了简明起见，这里不再对它们作详细说明.

一旦可执行对象（EO）经过了分析，那么对 EO 需要使用的计算机资源和安全策略所作的比较就很容易完成，例如，把它们和由 CC 提供给网关的、代表其安全策略的查阅表相比较. 比较可以针对存储在 CC 中的数据来实施，在这种情况下，在网关中就可以不一定需要特定的存储装置和比较装置. 不过，在速度和性能方面的考虑通常将要求这些操作应在网关本身内实现.

现有技术的解决方案所提供的对通信的分析是通过单独一个端口（即端口 80）实现的，这个端口通常是用于网络冲浪的端口．但是，现在已可通过除端口 80 以外的其它端口在网上冲浪，而按照当前可以利用的技术，用户的 HTTP 服务器不能工作在多个端口上．因此，如果有不止一个用户同时使用一个网关，现有技术的系统将不能工作，因为它们不适宜于同时分析通过其它端口所发生的通信．

另外一个严重缺点是，当按照现有技术的方法操作时，需要一个极其强大的 HTTP 服务器来为多个用户服务．

迄今为止这种技术还未能提供一个有效的方法来处理 EO，这种有效的方法和所用的端口无关，而且它也不需要去建立一个特别强大的服务器．因此很清楚，需要这样的解决方法，特别是考虑到许多单位正在不断增加对网络的使用．

发明概要

本发明的一个目的是提供一种处理可执行对象的有效方法，它克服了以前技术的系统的各种缺点．

本发明的另一目的是提供这样一种方法，它易于实现并且不需要明显改变硬件．

本发明的再一个目的是提供一种方法，它允许“在飞行中”（on the fly）分析可执行程序，并且不会影响无害的可执行程序的下载和操作．

本发明另外有一个目的是提供实现本发明的方法的设备．

本发明的其它优点和目的将随着说明的深入而更加明显．

本发明主要是针对一种处理可执行对象的方法，包括：

(a) 提供分析装置，它能够对在浏览器和网上的 HTTP 服务器之间的通信线路上发送的数据分组进行无干扰的分析，所说的通信线路是通过网关而建立的；

(b) 分析在上述浏览器和上述服务器之间的联络信号，以检测由用户送出的“GET_”命令和由上述服务器作出响应而送出的 HTTP 代码．

(c) 当检测到这样的 HTTP 代码时，分析由上述服务器发送给上述浏览器的数据分组，其过程为：

(1) 提供排序装置以便把收到的无顺序的数据分组排

序，然后把它们以顺序的方式转发给标题检查装置；

(2) 检查数据分组以便分析可执行对象的标题的内容，并识别它所需要使用的系统资源；

(3) 将表示可执行对象所需要使用的系统资源的数据发送给上述网关；以及

(4) 提供连接到上述网关的数据分组封锁装置，使得如果按照由管理者设置的安全策略不允许使用可执行对象所需要使用的系统资源时，至少一个属于可执行对象的数据分组被封锁、改变或损坏，从而防止它被浏览器所执行.

按照本发明的优选实施例，这个方法还包括识别通过网关进行通信的用户和上述用户所连接的服务器，并且把所有的活动和分析都与上述用户相联系. 这个步骤在有不止一个用户同时经过网关而连接时是必要的. 这样，多个用户连接到多个服务器. 因此，就有必要在某个用户向某一特定服务器请求特定的可执行对象的情况下跟踪该特定用户，以便正确地处理从任何个别服务器发来的在网关收到的分组.

在本发明的另一个优选实施例中，这个方法还包括在存储装置中存入表示被分析的可执行对象的校验和，与其一起存放的还有表示任何这样的可执行对象是否符合安全策略的值，并且在分析它之前或分析它的同时，针对该存放的值检查任何进入的可执行对象，以此来丢弃任何被判定为不符合安全策略的可执行对象，而让被判定为遵守安全策略的可执行对象通过网关而到达用户. 对于熟练的人员来说将会很明显，即这个过程可以使对可执行对象的分析变得流线化并得到加速，因为验证校验和是一种要比完整地分析 EO 的标题的过程更为快捷和更为简单的过程.

附图简述

在图中:

图 1 是按照本发明的优选实施例的、经过网关的、在浏览器和在网上的 HTTP 服务器之间并包括外加的分析装置的通信模式的原理示意图；和

图 2 说明按照本发明的优选实施例的、在处理数据分组方面存在于分析装置中的情况.

优选实施例的详细说明

本发明的方法现在将参考它的优选实施例而加以说明．在图 1 中表示了典型的情况，在该图中，浏览器 BR（运行在最终用户的计算机上）通过网关 GW 而连接到网络上．在图 1 中为了简单起见，只显示了一个浏览器，而实际上网关 GW 当然是设计来为多个浏览器服务的．与此相似，显示的网关 GW 也是只连接到网（表示为“WEB”）上的一个 HTTP 服务器，当然它可以连接到网上的多个服务器，而且其连接不是点到点的连接。

按照本发明的优选实施例，还提供了分析装置 L，它在一端连接到通信线路，而另一端则连接到网关．分析装置 L 是个被动装置，它只能“侦听”在浏览器 BR 和服务器 WEB 之间的在线路上发生的交谈．另外 L 还能够向网关 GW 发出一个信号．

浏览器和 HTTP 服务器之间的数据通信是以小型分组进行的，它们的综合构成了一个整体，这可以是也可以不是可执行对象．分组并不一定要按顺序发送，这一事实使它更加难于分析它们．从 WEB 到 BR 的分组发送是浏览器和 HTTP 服务器之间所实施的信号交换的结果．可执行对象的下载是用户送出一个含有“GET_”命令的消息的结果，这个命令在信号交换中由 HTTP 服务器回送，作为响应，该 HTPP 服务器在所请求的 EO 前送出一个 HTTP 代码．

这样，根据本发明，在识别所发送的数据是否为潜在有害的可执行对象的过程中的第一步是分析由 HTTP 服务器（WEB）发送的开头 4 个字节，并确定它们是否含有采用 HTTP 代码形式、对由用户送出的“GET_”命令的回答．如果有，那么，发送出的字串的剩余部分也必须进行分析以确定它是否含有 Java 应用程序或其它不需要的 EO．对分组进行处理的方法将在下面进一步说明．

如果像上面讨论的那样，分析装置 L 确定了涉及到可执行对象，那么必须对 EO 的标题作分析以检查它和由用户所规定的安全策略的一致性．这里必须再次强调，分析装置 L 只是“侦听”而并不干扰字串的发送。

分析装置包括不同的功能元件．在第一部分，收到的分组被存储并按顺序排列，以便让它的标题能得到分析．在图 2 中具有原理性的表示，其中可以看出分析装置 L 包括排序装置 OM，它在分组被发送时

接收它们，把它们排序并把它们以正确的次序传送．例如在图中的例子中可以看到，已经发送了6个分组，其次序为2、1、3、8、5、10．分组1、2、3被排成顺序并送往检查器CH，但是由于分组4还没有发送，所以剩余的分组（5、8、10）仍保存在OM中，一直到它们能被释放为止．分组5只有在分组4到达以后才能释放．而分组8则仅在分组6和7到达后才能释放，以此类推．这里应该再次强调，这种在OM中发生的延迟并不影响在浏览器BR和HTTP服务器WEB之间所发生的事务处理，所有的分组都会以它们未经排序的次序正常发送．但是，本发明利用这样一个事实，即使分组仍在继续发送，但如果有一个分组丢失或损坏，那么EO就不能工作．因此，当网关一旦确实从检查器收到一个信号，表明EO的标题中含有按照它的安全策略应该被禁止的命令，那么网关所关心的只是封锁或损坏一个分组就已足够．这样，按照本发明，数据的发送是不受干扰的，分组的分析是在无干扰的方式下进行的，而且发送只是受到是否希望防止EO在最终用户的计算机上运行的影响．本发明的方法的另一个优点是，需要作分析的只是在其前面带有对“GET_”命令的回答的数据，而且任何需要分析的字串只要达到能够确定它并不含有不需要的EO的那一点就可以了．

如上所述，按照本发明的优选实施例，如果可执行对象需要使用的计算机资源包含在安会策略允许使用的资源清单之内，那么系统就不必采取任何步骤来防止可执行对象经过网关而到达启动其下载的计算机．但是，如果可执行对象需要使用的计算机资源包含在被安全策略禁止使用的资源清单之内，那么将采取措施来防止可执行对象通过网关．这样的措施可以包括，例如，删除EO的一个分组，或者窜改它的一部分，从而使它不能工作，等等．

本发明并不局限于任何特定的EO．不过，按照本发明的优选实施例，尤其希望进行分析的EO包括：Java应用程序、ActiveX、OCX、Win32可执行程序、DLL，以及其它类似可执行对象．但是，对于熟悉的人员而言，很明显，EO是在不断发展的，本发明的意图决不限制在使用于特定的EO，并且EO的实际性质并不是关键性的重要问题．

优选实施例的所有上述说明都是作为实例而提供的，它并不用来以任何方式限制本发明，本发明只由权利要求所限定．本发明可以实

现许多修改. 例如, 可以监控多种不同的可执行对象, 可以应用不同的排序装置和分析装置, 同样也可以有不同的标题分析方法, 所有这些都不超出本发明的范围.

说 明 书 附 图

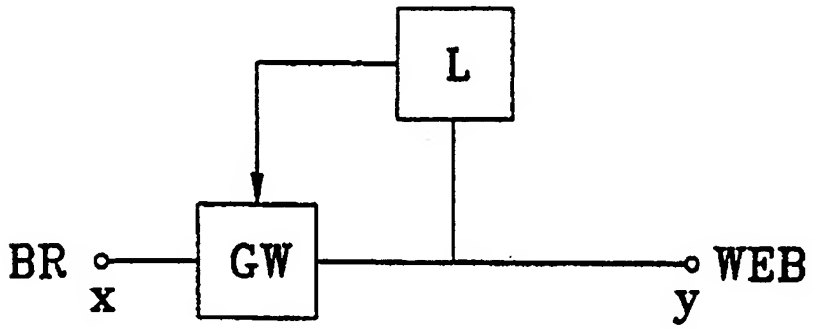


图 1

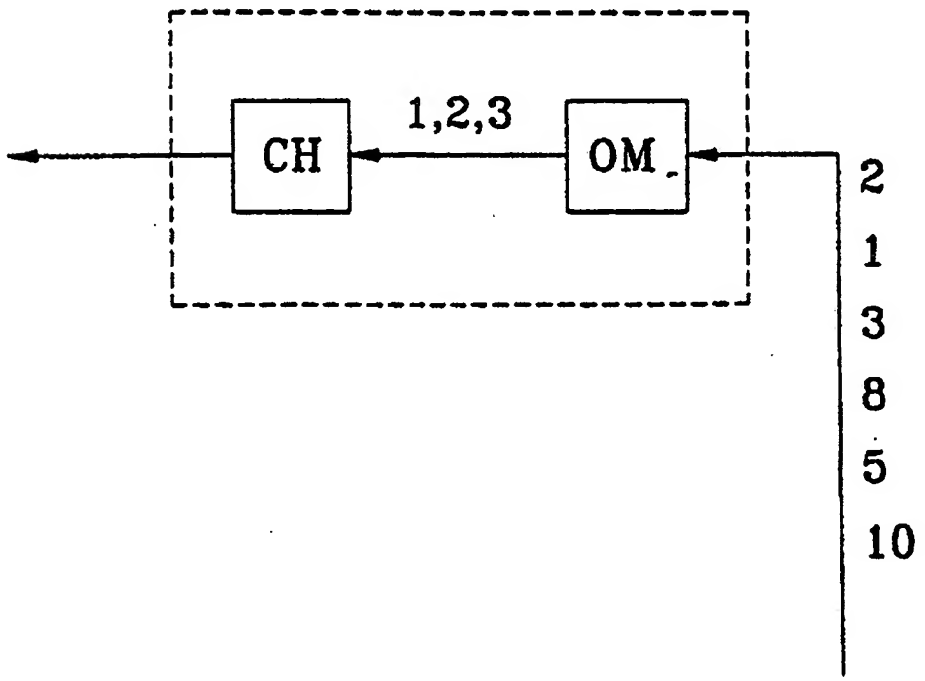


图 2